ABSTRACT

In a computer system with an operating system that supports multiple levels of interfaces (APIs) that application programs (i.e. programs executing outside the operating system kernel in user mode) can invoke to obtain services from the operating system, and the employment of a hooking or mediation technology within a user-mode process (i.e. an instantiation of an application program) to intercept/mediate invocations of selected interfaces of some of those levels, the Tampering Protection protects the code and statically or heap allocated data of the mediators from corruption by the code of the user-mode process being mediated that resides and operates in the same address space as the code and data of the mediators (as such corruption would compromise the integrity of the mediator and could prevent it from accomplishing its intended mediation purpose). It does so by providing memory protection services that allow mediators to define data areas (both static segments and dynamic heaps) to be protected and to temporarily unprotect them during the execution of a mediator so that they can be modified during that execution, thus ensuring that the mediate application does not directly use the operating system services to override Tampering Protection management of these protected segments or protected.